В. Ю. Попов
Уральский федеральный университет
им. первого Президента России Б. Н. Ельцина
Екатеринбург, Россия

Обнаружение обманных действий других роботов для повышения производительности

В последние годы значительно возросло количество атак нулевого дня. Атаки против киберфизических систем являются особенно опасными. Робототехнические системы отличаются наибольшей уязвимостью для атак нулевого дня среди таких систем. В работе рассмотрены способы обнаружения обманных атак со стороны других роботов для повышения собственной производительности робота. Особое внимание уделено атакам, связанным с имитацией действий людей. Проанализирована активная система обнаружения обманных атак нулевого дня. На основе экспериментальных данных произведено сравнение эффективности активного и пассивного обнаружения, а для атакующей системы — эффективности имитационного подхода и использования произвольных обманных атак.

Ключевые слова: мобильный робот, искусственный интеллект, обманные действия, атаки нулевого дня, робот-гуманоид

Vladimir Yu. Popov
Ural Federal University
named after the first President of Russia B. N. Yeltsin
Yekaterinburg, Russia

The Discovery of Deceptive Actions of Other Robots to Increase Performance

The number of zero-day attacks has increased significantly in recent years. Attacks against cyber-physical systems are particularly dangerous. Robotic systems are the most vulnerable to zero-day attacks among cyber-physical systems. We pay special attention to attacks related to imitation of human actions. We consider an active detection system for zero-day

deceptive attacks. In our experiments for the detection system, we have compared the efficiency of active and passive detection, for the attacking system — the effectiveness of the imitation approach and the use of arbitrary deception attacks.

Keywords: mobile robot, artificial intelligence, deceptive actions, zero-day attacks, humanoid robot

Введение. На фоне общего роста атак нулевого дня [1] особенно ярко выделяются атаки, направленные на киберфизические системы [2]. В последние годы наибольшее увеличение уязвимостей и угроз наблюдается для систем индустриального Интернета вещей [3]. В частности, быстрое развитие Интернета транспортных средств значительно повышает угрозу различных типов обманных атак против автономных роботов [4]. Обманные атаки нулевого дня являются одной из наиболее опасных и трудно идентифицируемых разновидностей деструктивной активности, которая может быть направлена против киберфизических систем. Особенно для этих атак уязвимы автономные робототехнические комплексы. Причина этому кроется в необходимости, располагая автономностью, полностью повиноваться воле людей: роботы могут атаковать других роботов, имитируя действия людей. Общая задача обнаружения обманных атак является слишком объемной и многогранной. Поэтому в рамках данного исследования мы ограничимся лишь рассмотрением вопроса обнаружения обманных атак со стороны других роботов для повышения собственной производительности робота. Особое внимание предполагается уделить атакам, связанным с имитацией действий людей.

Материалы и методы. Нами рассмотрена модель взаимодействия группы роботов. В рамках этой модели мы предполагаем, что только один робот может использовать обманные действия. Все роботы должны решать свои собственные задачи, которые могут требовать взаимодействия. В частности, некоторые задачи могут быть решены лишь совместными усилиями. Для проведения экспериментов в качестве потенциально атакуемых роботов рассматривались только мобильные роботы. В качестве атакующего робота мы использовали как мобильный робот, так и робот-гуманоид.

Результаты. Предложена активная система обнаружения обманных атак нулевого дня. Система не предполагает использования для обнаружения атак специализированных последовательностей действий, которые не связаны непосредственно с решением повседневных задач, поставленных перед роботом. Обнаружение атак основано на возможности выбора различных последовательностей действий, направленных на решение основных задач робота. Манипулируя способами решения своих задач, робот наблюдает за последствиями своих действий. Изучение последствий действий робота осуществляется по трем основным направлениям: анализ внешней активности, сравнение реальной эффективности действий с предполагаемой, мониторинг внутреннего состояния робота. Анализ внешней активности предполагает принятие во внимание не только активности других роботов, но и изменений окружения. Следует отметить, что при мониторинге внутреннего состояния робота тревожным сигналом считается не только ухудшение состояния, но и улучшение, не имеющее объективных предпосылок: был на заправке, прошел очистку, сделал калибровку и т. д. Основной акцент при генерации способами решения сделан на взаимодействии робота с другими роботами: отказ от предложенного взаимодействия, активное предложение взаимодействия, выбор момента взаимодействия, работа в непосредственной близости от других роботов, соблюдение заданной дистанции до других роботов и т. д. Учет возможности имитационных атак требует от системы обнаружения отдельной обработки. Как обычно, верификация человечности основана на использовании базы знаний. Однако использование активного обнаружения открывает дополнительные возможности, связанные с планированием упреждающего контакта, позволяющего осуществить верификацию до непосредственного начала атаки. При этом следует учитывать, что упреждающий контакт может спровоцировать незапланированную или более интенсивную атаку. Поэтому вместо непосредственного упреждающего контакта робот стремится осуществить косвенный упреждающий контакт, осуществляемый через окружение или других роботов. В рамках проведенных экспериментов мы сравнили эффективность активного и пассивного обнаружения. С атакующей стороны сравнивался

имитационный подход с использованием произвольных обманных атак. Для имитационного подхода мы рассматривали симуляцию как реальных действий человека, так и действий, построенных на основе последовательностей случайных чисел, сгенерированных человеком.

Заключение. Результаты исследований показали значительное преимущество активного обнаружения над пассивным. С атакующей стороны было выявлено существенное преимущество имитационного подхода. Однако эксперименты показали, что симуляция реальных действий человека может быть успешно заменена симуляцией действий, построенных на основе последовательностей случайных чисел, сгенерированных человеком. Более того, вместо последовательностей случайных чисел, сгенерированных человеком, могут успешно использоваться искусственные последовательности, созданные интеллектуальной системой, имитирующей генерацию человека.

1. *Khraisat A., Gondal I., Vamplew P., Kamruzzaman J.* Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity. 2019. Vol. 2. P. 1–22.

2. *Mitchell R., Chen I.-R.* A survey of intrusion detection techniques for cyber physical systems // ACM Computing Surveys. 2014. Vol. 46. P. 1–27.

3. Security and privacy trends in the industrial Internet of Things / ed. C. Alcaraz. Cham : Springer Nature Switzerland AG, 2019.

4. *Liu X., Jiang R., Wang H., Ge S. S.* Filter-based secure dynamic pose estimation for autonomous vehicles // IEEE Sens. J. 2019. Vol. 19. P. 6298–6308.